Cyber security researchers from 12 countries participated in the conference. Here, a member of the Blue Team shares expertise and helps the team gain an advantage protecting their chemical system from a cyber attack.

## International conference plays cyber war games

by Sara Prentice, INL Communications & Public Affairs

On the morning of April 2, a specialty chemical company came under cyber attack in a fictitious scenario. Aggressors hired by a competing company were trying to hack into the chemical processing systems. If the hackers succeeded, the company risked losing an early market share on a revolutionary chemical it planned to unveil. Teams at the chemical company worked tirelessly for the next 12 hours to defend the network and company secrets from attack.

This scenario was developed by the U.S. Department of Homeland Security (DHS) as part of an industrial control systems exercise to simulate real threats facing our nation's critical infrastructure, such as chemical facilities, power plants and communications networks. At the recent 2009 International Control Systems Cyber Security Advanced Training, sponsored by the DHS, the Control Systems Security Program (CSSP) worked to raise cyber awareness with the international community about the threats facing critical infrastructure.

***Members of the Red Team, hoping to get ahead in the cyber war game, work together trying to find weaknesses in the Blue Team's network.***

During the first week of April, top cyber security researchers and infrastructure protection specialists from 12 countries came to the DHS Control Systems Analysis Center, located at the U.S. Department of Energy's Idaho National Laboratory (INL), to participate in a comprehensive, cyber security training. Participants represented the United States, Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, Netherlands, New Zealand and Sweden.

The 40 attendees completed intensive hands-on training that focused on protecting and securing vital infrastructure from industrial control systems cyber attacks.

Sean McGurk, DHS CSSP program manager, said, "cyber security requires that organizations be diligent protecting their nation's critical infrastructure, and the exercise provides the experience in understanding the importance of the cyber risks to industrial control systems."

"Cyber security in not just an issue in the United States, but is also an international concern that requires collaboration with other countries," said Marty Edwards, INL program manager of the DHS Control Systems Security Program.

The five-day training event culminated in an industrial control systems exercise that provided friendly competition between a Red Team that is attacking the industrial control system of the Blue Team, whose goal is to defend against the cyber attacks.

***INL employee, Jared Verba, works behind the scenes keeping the cyber war game running smoothly.***

Exercise participants were split into the two teams. The nine members of the Red Team were tasked with attacking the fictional Specialty Chemical Company. The 23-member Blue Team task was to defend the network and the chemical facility from attack. A real-time scoring system was used so that both teams could obtain and use points based upon the defensive measures implemented (Blue Team) or information extracted (Red Team) during the 12-hour exercise.

Teams were scored by accomplishing their offensive and defensive goals and objectives. The Blue Team earned points by defending its networks, patching systems, detecting exploitation and malware, and manufacturing products. The Red Team earned points by successfully accomplishing offensive goals such as network scanning, network exploitation, theft of information and manipulation of the Industrial Control System network.

For the 2009 event, the Blue Team successfully defended the chemical facility from the Red Team attack. The Red Team, despite its loss, did launch several successful attacks, but was never able to completely shut down the specialty chemical process.

Participants left the event with a greater awareness of the threats facing critical infrastructure and expressed the importance of learning actionable mitigation measures that they will be able to apply to their work situations and share with others in their own countries.

Idaho National Laboratory is a U.S. Department of Energy (DOE) laboratory and supports the DHS CSSP and the DOE National Supervisory Control and Data Acquisition (SCADA) Test Bed programs. These government-sponsored programs view the Red/Blue Team Industrial Control Systems exercise as an important element in mitigating the risk to the nation's critical infrastructure, and they are scheduled to host eight additional trainings in 2009.

For more information on the DHS CSSP and the control systems security trainings, visit http://www.us-cert.gov/control_systems/.

Feature Archive